APPLICATION

FOR

UNITED STATES LETTERS PATENT

TITLE: **AUTOMATED GLOBAL RISK MANAGEMENT**

APPLICANT: **David Lawrence**

"EXPRESS MAIL" Mailing Label Number EL478577945US

Date of Deposit March 20, 2001.
I hereby certify under 37 CFR 1.10 that this correspondence is being deposited with the United States Postal Service as **"Express Mail Post Office to Addressee"** with sufficient postage on the date indicated above and is addressed to the Assistant Commissioner for Patents, Washington, D.C. 20231.

James Porter

James Porter

AUTOMATED GLOBAL RISK MANAGEMENT

BACKGROUND

This invention relates generally to a method and system for facilitating the identification, investigation, assessment and management of legal, regulatory financial and reputational risks ("risks"). In particular, the present invention relates to a computerized system and method for banks and non-bank financial institutions to access information compiled on a worldwide basis, wherein the information is conducive to quantifying and managing financial, legal, regulatory and reputational risk.

Bank and non-bank financial institutions, including: investment banks; merchant banks; commercial banks; securities firms, including broker dealers securities and commodities trading firms; asset management companies, hedge funds, mutual funds, credit rating funds, securities exchanges and bourses, institutional and individual investors, law firms, accounting firms, auditing firms and other entities, hereinafter collectively referred to as "financial institutions," typically have few resources available to them to assist in the identification of present or potential risks associated with business transactions. Risk can be multifaceted and far reaching. Generally, personnel do not have available a mechanism to provide real time assistance to assess a risk factor or otherwise qualitatively manage risk. In the event of problems, it is often difficult to quantify to regulatory bodies, shareholders, newspapers and other interested parties, the diligence exercised by the financial institution to properly identify and respond to risk factors. Absent a means to quantify good business practices and diligent efforts to contain risk, a financial institution may appear to be negligent in some respect.

Risk associated with maintaining an investment account can include factors associated with financial risk, legal risk, regulatory risk and reputational risk. Financial risk includes factors indicative of monetary costs that the financial institution may be exposed to as a result of opening a particular account and/or transacting business with a particular client. Monetary costs

can be related to fines, forfeitures, costs to defend an adverse position, or other related potential sources of expense. Regulatory risk includes factors that may cause the financial institution to be in violation of rules put forth by a regulatory agency such as the Securities and Exchange Commission (SEC). Reputational risk relates to harm that a financial institution may suffer regarding its professional standing in the industry. A financial institution can suffer from being associated with a situation that may be interpreted as contrary to an image of honesty and forthrightness.

Risk associated with an account involved in international transactions can be greatly increased due to the difficulty in gathering and accessing pertinent data on a basis timely to managing risk associated with the transaction. As part of due diligence associated with managing financial accounts, it is imperative for a financial institution to "Know Their Customer" including whether a customer is contained on a list of restricted entities published by the Office of Foreign Access Control (OFAC), the Treasury Office or other government or industry organization.

Compliance officers and other financial institution personnel typically have few resources available to assist them with the identification of present or potential global risks associated with a particular investment or trading account. Risks can be multifaceted and far reaching. The amount of information that needs to be considered to evaluate whether an international entity poses a significant risk or should otherwise be restricted, is substantial.

However, financial institutions do not have available a mechanism which can provide real time assistance to assess a risk factor associated with an international entity, or otherwise qualitatively manage such risk. In the event of investment problems, it is often difficult to quantify to regulatory bodies, shareholders, newspapers and/or other interested parties, the diligence exercised by the financial institution to properly identify and respond to risk factors. Absent a means to quantify good business practices and diligent efforts to contain risk, a financial institution may appear to be negligent in some respect.

What is needed is a method and system to draw upon information gathered globally and utilize the information to assist with risk management and due diligence related to financial

accounts. A new method and system should anticipate offering guidance to personnel who interact with clients and help the personnel identify high risk situations. In addition, it should be situated to convey risk information to a compliance department and be able to demonstrate to regulators that a financial institution has met standards relating to risk containment.

SUMMARY

Accordingly, the present invention provides a risk management method and system for facilitating analysis and quantification of risk associated with a financial transaction. An automated global risk management system maintains a database relating risk variables including world events government advisories, and other information sources with potential risk for a financial institution. A rating system is used to assess risk based upon criteria such as risk advisories, historical data and/or interpretation of world events. The system can generate a risk quotient or other rating based upon a weighted algorithm applied to the criteria, wherein the risk quotient is indicative of risk associated with a transaction or an account. The quotient can be monitored on a periodic basis, during the course of a transaction, upon account opening or on demand. Actions commensurate with a risk quotient can be presented to a financial institution to help the institution properly manage risk associated with a particular entity or transaction.

A log or other stored history can be created such that utilization of the system can mitigate adverse effects relating to a problematic account. Mitigation can be accomplished by demonstrating to regulatory bodies, shareholders, news media and other interested parties that corporate governance is being addressed through tangible risk management processes. In summary fashion, the present invention includes a method and system for identifying risks associated with the domestic and global commercial activities of financial firms including, for example, a transactions involving: financial institution, an insurance company, a credit card issuer, a trading exchange, a government regulator, a law enforcement agency, an investment and merchant bank, public and private financing, commodities and securities trading, commercial and consumer lending, asset management, the ratings of corporations and securities, public and private equity investments, public and private fixed income investments, the listing of companies

on securities exchanges and bourses, employee screening and hereinafter collectively referred to as "Financial Transactions."

In another aspect, a computer system for providing risk management relating to opening accounts can include a computer server that is accessible with a network access device via a communications network and executable software stored on the server which is executable on demand via the network access device. The software can be operative with the server to gather or receive information relating to risk factors and formulate a risk quotient or other rating. In addition, where applicable, risk can be aggregated, such as by rating, and transferred.

The present invention includes a computer-implemented method for managing risk related to financial transactions involving international or global exposure. The method includes receiving information relating to an entity involved in a financial transaction and structuring the information received according to risk quotient criteria. A risk quotient is calculated using the structured information. A suggested action responsive to the risk quotient or the information received can also be generated.

Typically the suggested actions will be directed towards reducing risk relating to an account associated with international exposure, although actions can be directed towards law enforcement or other directives also. In one embodiment, the action can include refusing to open an account or perform a transaction. Another action may involve notifying an authority, such as the police.

In another aspect, the information received can be stored, as can the risk quotient and the suggested action, and utilized to generate a diligence report. The diligence report can include information received relating to an account and actions taken responsive to the risk quotient.

Still another aspect can include aggregating risk quotients relating to a financial institution to assess a level of identified risk to which the financial institution is exposed. An average risk quotient associated with a transaction can also be calculated.

Other embodiments include a computerized system for managing risk associated with a financial account, computer executable program code residing on a computer-readable medium, a computer data signal embodied in a digital data stream, or a method of interacting with a

network access device. Various features and embodiments are further described in the following figures, drawings and claims.

DESCRIPTION OF THE DRAWINGS

Fig. 1 illustrates a block diagram that can embody this invention.

Fig. 2 illustrates a network on computer systems that can embody an automated global risk management system.

Fig. 3 illustrates a flow of exemplary steps that can be executed by a GRM system.

Fig. 4 illustrates a flow of exemplary steps that can taken by a user of the GRM system.

Fig. 5 illustrates an exemplary graphical user interface useful for gathering information according to the present invention.

Fig. 6 illustrates an exemplary graphical user interface useful for presenting reports related to GRM.

DETAILED DESCRIPTION

The present invention includes a computerized method and system for managing risk associated with financial transactions with international exposure. A computerized system gathers and stores information in a database or other data storing structure and relates the information to risk factors pertaining to financial accounts. A rating system is used to assess risk based upon the information received and the risk factors. A rating, such as a risk quotient can be generated too readily indicate a level of risk associated with a particular account or account holding entity. The risk quotient can be based upon a weighted algorithm applied to the risk factors. The risk quotient can be made available on a periodic basis, on demand in real time, in response to an event such as an account opening, or according to some other request. Actions commensurate with a risk level can be presented to assist with proper risk management.

Referring now to Fig. 1 a block diagram of one embodiment of the present invention is illustrated. A Global Risk Management (GRM) system 106, receives information relating to entities that are restricted, controlled, or otherwise marked as high risk. The information can be received for example from a list generated by the Office of Foreign Assets Control (OFAC) 101

including their sanction and embargo list, a list generated by the U.S. Commerce Department 102, a list of international "kingpins" generated by the U.S. White House 103, U.S. regulatory actions 104 or other information source 105 such as a foreign government, US adverse business-related media reports, US state regulatory enforcement actions, International regulatory enforcement actions, International adverse business-related media reports, a list of politically connected individuals and military leaders, list of U.S. and international organized crime members and affiliates or a list of recognized high risk countries. Other information received may indicate that an entity is not high risk. For example an entity may be a corporation from a G-7 country that is traded on a major exchange.

Information can also be input by a financial institution. For example, in the course of dealings with a particular entity, a financial institution may discover or suspect that the entity is involved in some fraudulent or otherwise illegal activity and report this information to the GRM system 106.

A decision by a financial institution concerning whether to pursue a financial transaction can be dependent upon many factors. A multitude and diversity of risks related to the factors may need to be identified and evaluated. In addition, the weight and commercial implications of the factors and associated risks can be interrelated. The present invention can provide a consistent and uniform method for business, legal, compliance, credit and other personnel of financial institutions to identify and assess risks associated with a transaction. A GRM system 106 allows investment activity risks to be identified, correlated and quantified by financial institutions thereby assessing legal, regulatory, financial and reputational exposure.

Financial institutions are often closely regulated. As a result financial institutions are exposed to significant risks from their obligations of compliance with the law and to prevent, detect and, at times, report potential violations of laws, regulations and industry rules ("laws"). These risks include, but are not limited to, the duty to disclose material information, and to prevent and possibly report: fraud, money laundering, foreign corrupt practices, bribery, embargoes and sanctions. Through a series of structured questions and weighting of information received as answers, financial institutions can structure a risk exposure and receive suggested responses to a specific risk scenario.

A financial institution can integrate a GRM system 106 as part of legal and regulatory oversight for various due diligence and "know your customer" obligations imposed by regulatory authorities. The GRM system 106 can facilitate detection and reporting of potential violations of law as well as address the "suitability" of a financial transaction and/or the assessment of sophistication of a customer. Similarly, the GRM system 106 can support a financial institution's effort to meet requirements regarding the maintenance of accurate books and records relating to their financial transactions and affirmative duty to disclose material issues affecting an investor's decisions.

An institution that may implement, or make use of the present invention can include an investment bank, a merchant bank, a commercial bank, a security firm, an asset management company, a hedge fund, a mutual fund, a credit rating agency, a security exchange and bourse, an institutional or individual investor, an auditing firm, a law firm, or other institution who may be involved with financial transactions. Similarly, financial investments can include investment and merchant banking, public and private financing, commodities and a securities trading, commercial and consumer lending, asset management, rating of corporations and securities, public and private equity investment, public and private fixed income investment, listing to companies on a securities exchange and bourse, employee screening, auditing of corporate or other entities, legal opinions relating to a corporate or other entity, or other business related transactions.

A log or other stored history can be created such that utilization of the system can mitigate adverse effects relating to a problematic account. Mitigation can be accomplished by demonstrating to regulatory bodies, shareholders, news media and other interested parties that corporate governance is being addressed through tangible risk management processes. An implementing institution may include, for example, a bank, a trading institution, an insurance company, a credit card issuer, a trading exchange, a government regulator or a law enforcement agency.

Information relating to financial, legal, regulatory and/or reputational risk is received into a computer system. The computer system applies an algorithm that weights the input

information and calculates a risk quotient or similar score or rating. The risk quotient can include, for example, a scaled numeric or alpha-numeric value.

If an account reaches or exceeds a risk quotient threshold, the system responds with a predetermined action. Actions can include, for example, generating an alert, blocking acceptance of a transaction, creating a report, notifying a compliance department, or other appropriate response. In addition, the system can create a structured history relating to a new account that can demonstrate due diligence and proper corporate governance. Reporting can be generated from the structured history.

In the case of an automated account opening, such as, for example, opening an online account, questions can be presented to the account opener by a programmable robot via a GUI. Questions can relate to a particular type of account, a particular type of client, types of investment, or other criteria. Other prompts or questions can aid a financial institution ascertain the identity of an account holder and an account's beneficial owner. If there is information indicating that a proposed account is beneficially owned by a high risk entity, the financial institution may not wish to open an account if it is unable to determine the identity of the high risk entity and his or her relationship to the account holder.

The GRM system 106 can receive open queries containing information relating to an individual or circumstance associated with a financial transaction and/or provide questions, historical data, world event information and other targeted information to facilitate a determination regarding an at risk entity's source of wealth and of the particular funds involved with an account or transaction in consideration.

Questions or prompts proffered by the GRM system 106 can also depend from previous information received. Information generally received, or received in response to the questions, can be input into the GRM system 106 from which it can be utilized for real time GRM risk assessment and generation of a GRM risk quotient 108.

The GRM risk assessment and GRM risk quotient 108 can subsequently be made available by the GRM system 106 to a financial institution 111 or personnel interested in the transaction 107. In one embodiment, the GRM risk quotient can be made available in real time. A real time assessment can allow the GRM system 106 to provide a suggested action, which can

be taken to address a particular risk quotient. The GRM system 106 can also take into consideration input information in order to generate a suggested action. A suggested action may include; for example, limiting the scope of a transaction entered into, discontinuing a transaction associated with high risk participants, notifying authorities, or other appropriate actions.

The GRM system 106 can quantify risk due diligence 109 by capturing and storing a record of information received and actions taken relating to a GRM account. Once quantified, the due diligence data can be utilized for presentation to regulatory bodies, shareholders, news media and/or other interested parties, to mitigate adverse effects relating to a problematic account. The data can demonstrate that corporate governance is being addressed through tangible risk management processes.

The GRM system 106 can also aggregate risk quotient scores 108 to assess a level of GRM risk being tolerated by the institution. Other calculations, such as, for example, the sum, mean, average, or other calculation can be made by the GRM system 106 to further analyze GRM risk at a financial institution. If desired, a rating can be applied to an institution according to the amount for GRM risk tolerated by the institution, such as, for example, the average risk tolerated.

Referring now to Fig. 2, a network diagram illustrating one embodiment of the present invention is shown. An automated GRM system 106 can include a computerized GRM server 210 accessible via a distributed network 201 such as the Internet, or a private network. A client 220-222, regulatory entity 226, compliance entity 223, account opening personnel 224, or other party interested in GRM risk management, can use a computerized system or network access device 204-208 to receive, input, transmit or view information processed in the GRM server 210. A protocol, such as the transmission control protocol internet protocol (TCP/IP) can be utilized to provide consistency and reliability.

Each network access device can include a processor, memory and a user input device, such as a keyboard and/or mouse, and a user output device, such as a display screen and/or printer. The network access devices 204-208 can communicate with the GRM server 210 to access data stored at the GRM server 210. The network access device 204-208 may interact with

the GRM server 210 as if the GRM server 210 was a single entity in the network 200. However, the GRM server 210 may include multiple processing and database sub-systems, such as cooperative or redundant processing and/or database servers, that can be geographically dispersed throughout the network 201. In some implementations, groups of network access devices 204-208 may communicate with GRM server 210 through a local area network.

The GRM server 210 includes one or more databases 202 storing data relating to GRM risk management. The GRM server 210 may interact with and/or gather data from an operator of a network access device 204-208, such as a client 220-222, compliance entity 223, account opening personnel 224, regulatory entity 226, or other person in control of the device 204-208. Data gathered from an operator may be structured according to risk criteria and utilized to calculate a GRM risk quotient 108.

Typically an operator or other user will access the GRM server 210 using client software executed at a network access device 204-208. The client software may include a generic hypertext markup language (HTML) browser, such as Netscape Navigator or Microsoft Internet Explorer, (a "WEB browser"). The client software may also be a proprietary browser, and/or other host access software. In some cases, an executable program, such as a Java™ program, may be downloaded from the GRM server 210 to the client computer and executed at the client network access device or computer as part of the GRM system software. Other implementations include proprietary software installed from a computer readable medium, such as a CD ROM. The invention may therefore be implemented in digital electronic circuitry, computer hardware, firmware, software, or in combinations of the above. Apparatus of the invention may be implemented in a computer program product tangibly embodied in a machine-readable storage device for execution by a programmable processor; and method steps of the invention may be performed by a programmable processor executing a program of instructions to perform functions of the invention by operating on input data and generating output.

Referring now to Fig. 3, steps taken to manage risk associated with a financial transaction with global risk exposure can include gathering information relating to risk entities and other risk variables. Informational data can be gathered from a user or from a source of electronic data such as an external database, messaging system, news feed, government agency, or other

automated data provider. Typically, the GRM system 106 will receive data relating to a potential account holder, beneficiary or other associated party. Information can be received on an ongoing basis such that if new events occur in the world which affect the political exposure of an account holder, the GRM risk can be adjusted accordingly.

In addition to the types and sources of information listed previously that can provide indications of high risk, the financial institution or compliance entity can receive information that relates to requests to involve a financial institution that is not accustomed to foreign account activity; requests for secrecy or exceptions to Bank Secrecy Act requirements, routing through a secrecy jurisdiction, or missing wire transfer information; unusual and unexplained fund or transaction activity, such as fund flow through several jurisdictions or financial institutions, use of a government-owned bank, excessive funds or wire transfers, rapid increase or decrease of funds or asset value not attributable to the market value of investments, high value deposits or withdrawals, wires of the same amount of funds into and out of the account, and frequent zeroing of account balance; and large currency or bearer transactions, or structuring of transactions below reporting thresholds. Other information can include activities the GRM is involved in, associates of the GRM, governmental changes, or other related events.

Sources of information can include, for example, publications issued by Treasury's Financial Crimes Enforcement Network ("FinCEN"), the State Department, the CIA, the General Accounting Office, Congress, the Financial Action Task Force ("FATF"), various international financial institutions (such as the World Bank and the International Monetary Fund), the United Nations, other government and non-government organizations, internet websites, news feeds, commercial databases, or other information sources.

The GRM server 210 can structure the information received according to defined GRM risk quotient criteria 312. For example, information received can be associated with criteria including a position held by the account holder, the country in which the position is held, how long the position has been held, the strength of the position, the veracity of previous dealings with persons from that country, the propensity of people in similar positions to execute unlawful or unethical transactions, the type of account or other criteria.

Types of accounts to be opened may include, for example: an individual account, a public company domiciled in a G-7 country or Hong Kong, a public company not domiciled in a G-7 country or Hong Kong, a corporate account regulated by a G-7 agency or a corporate account regulated by a non G-7 government agency, a private company or partnership, a holding company, an intermediary managed account such as a money manager or hedge fund, a trust or foundation, or other type of legal entity.

The GRM server 210 can receive information and structure it according to predefined criteria or receive it in a pre-structured format. Receiving the information in a pre-structured format allows the GRM server 210 to proceed with calculating a risk quotient 313 without having to further structure the information. Information that cannot be easily structured can also be received and archived in order to facilitate a manual qualitative evaluation.

A GRM risk quotient can be calculated 313 by weighting the information received according to its importance in determining high risk activities, such as the likelihood of illegal or unethical dealings. Calculating a GRM risk quotient can be accomplished by assigning a numerical value to each field of information, wherein the numerical value is representative of the risk associated with a particular piece of information. For example, it may be determined in one case that a government official from a G-7 country trading equities in a public company from a G-7 country poses minimal risk. Therefore this information from the first case is assigned a low numerical value, or even a negative numerical value. In a second case, an individual who appears on a list generated by the FATF and is attempting to transact in a corporate holding company may be viewed as a high risk. In another case, information conveying this high risk may be assigned a high numerical value. In addition, a weight can be assigned to a GRM risk category to which the information is assigned. Therefore a designated country may receive a higher weight than the position held, or vice versa. A Risk Quotient can be calculated by multiplying a weighted numerical value of the specific information times the category weighting.

For example, information received may indicate an account holder is a high ranking finance official from a G7 country. The ownership structure of a company the account holder wishes to transact is a public entity. A public entity may receive a numerical value of –5 because it is a relatively low risk ownership structure. In addition, this information may be included in a

Company Profile category, wherein the Company Profile is assigned a category weighting of 3. Therefore, the net score for this ownership structure is –5 times 3 or –15. Similarly the account holder being a high ranking official from a G-7 country may also receive a low number such as 1. The GRM risk quotient for the account holder would be 1 times 3, or 3. All scores within the Company Profile can be summed to calculate a GRM risk quotient. In this case the GRM risk quotient is –15 + 3 which equals –12, indicating a low risk. Weighted risk scores from all associated categories can be summed to calculate a total Risk Quotient Score 108.

A suggested action can be generated that is responsive to the Risk Quotient 314. For example, in response to a high risk score a suggested action may be to not proceed with a transaction, or even to notify an authority. In response to a low risk score, the GRM server 210 may respond by completing transactions as usual. Intermediate scores may respond by suggesting that additional information be gathered, that transactions for this account be monitored, or other interim measures.

The GRM server 210 can also store, or otherwise archive GRM data and proceedings. For example the GRM server 210 can store information received, a Risk Quotient generated, and also the suggested actions to be taken 315. This information can be useful to quantify corporate governance and diligent efforts to address high risk situations. Accordingly, reports quantifying GRM risk management procedures, executed due diligence, corporate governance or other matters can be generated 316.

Referring now to Fig. 4, a flow chart illustrates steps that a user, such as a financial institution, can implement to manage risk associated with a transaction. The user can receive information relating to an entity associated with a transaction 410. This information may be received during the normal course of business, such as when the participants to a transaction are ascertained. The user can access a GRM server 210 and identify to the GRM server 210 one or more entities, jurisdictions, or other risk variables involved in the transaction 411. Access can be accomplished by opening a dialogue with a GRM system. Typically, the dialogue would be opened by presenting a GUI to a network access device accessible by a person or an electronic feed that will enter information relating to the account holder. The GUI will be capable of accepting data input via a network access device. An example of a GUI would include a series

of questions relating to a client holding an account. Alternatively, information can be received directly into fields of a database, such as from a commercial data source. Questions can be fielded during a transaction, while updating account information, during an account opening interview, or at any other opportunity to gather information.

In one embodiment, automated monitoring software can run in the background of a normal transaction program and screen data traversing an application. The screened data can be processed to determine key words wherein the key words can in turn be presented to the GRM server 210 as risk variables. The GRM server 210 will process the key words to identify entities or other risk variables and score those variables according to weighted criteria. Monitoring software can also be installed to screen data traversing a network or communications link.

The user will receive back information relating to risk associated with conducting a transaction involving the submitted variables 412. The user will also receive a GRM Risk Quotient 413. As addressed more completely above, the risk quotient is typically a scaled numerical score based upon values for weighted criteria. It will represent a magnitude of risk associated with a particular transaction and can be based upon the participants involved in a transaction, the type of transaction, the state sovereignties involved, an amount of money involved in the transaction, or other risk variables.

In addition to receiving the GRM risk quotient 413, the user can also receive one or more suggested actions responsive to the risk quotient 414. A suggested action can include reasonable steps that can be taken by the financial institution or other user to address a risk that is associated with the transaction. The user can also archive information relating to risk associated with a transaction as well as steps taken to address the risk 415. The process involved in utilizing the GRM system can be included in the archive as steps taken to diligently manage risk associated with a global transaction.

The user can also generate reports to quantify the archived information and otherwise document diligent actions taken relating to risk management.

Referring now to Fig. 5, an exemplary GUI for displaying information related to GRM is illustrated 500. The GUI can include areas prompting for information, such as in the form of a key word or a question 501. Areas can also be included for an appropriate response 506. The

area for an appropriate response 506 can, for example, receive text, allow a selection from choices proffered, or otherwise receive data into the GRM server 210. A programmable user interactive device, such as a checkbox, X field, yes/no filed or other device 503-505 can also be utilized to indicate an answer, or otherwise input information. Other programmable devices, such as programmable icons, hyperlinks, push buttons or other devices 502 can also be utilized to execute a particular function. A category weighting area 507 can also be indicated on the GUI 500. Typically the weighting will be predetermined. However, if desired the weighting can be modified by a user such that a weighting value, such as a numerical value, will be utilized to calculate a risk quotient. The GRM GUI 500 can also include an area for displaying a quotient score relating to the transaction 508.

Referring now to Fig. 6, an exemplary GUI for presenting reports or suggested actions related to GRM is illustrated 600. The GUI for presenting reports 600 can include geographic areas of a user interface containing risk management procedures 601, including those procedures specifically followed in relation to a particular GRM or other suggested actions. Additional areas can include a list of electronic or hardcopy reports available concerning risk management efforts undertaken 602. Another area can include a list of risk quotients and./or calculations concerning a risk quotient, such as the average risk quotient for the financial institution, or the mean risk quotient 603. Still another area can contain information descriptive of a particular account holder or GRM 604.

A number of embodiments of the present invention have been described. Nevertheless, it will be understood that various modifications may be made without departing from the spirit and scope of the invention. For example, network access devices 204-208 can comprise a personal computer executing an operating system such as Microsoft Windows™, Unix™, or Apple Mac OS™, as well as software applications, such as a JAVA program or a web browser. network access devices 204-208 can also be a terminal device, a palm-type computer, mobile WEB access device, a TV WEB browser or other device that can adhere to a point-to-point or network communication protocol such as the Internet protocol. Computers and network access devices can include a processor, RAM and/or ROM memory, a display capability, an input device and hard disk or other relatively permanent storage. Accordingly, other embodiments are within the scope of the following claims.